MY SOCIAL ENGINEERING CHECKLIST

WHEN YOU RECEIVE AN EMAIL AND SOMETHING LOOKS UNUSUAL, ASK YOURSELF...

AM I USING COMMON SENSE?

Be wise to the threat. If opening the email or downloading the attachment doesn't feel right, don't do it. People that are too comfortable or complacent in this regard are prime targets.

IS THIS A PHISHING EMAIL?

Phishing emails get you to click a malicious link or open a malicious attachment using coercion tactics, such as urgency, e.g. "We're upgrading our servers, click this link to avoid all your emails being deleted." Don't fall into the phishing trap - recognise the signs and report them.

HAVE I VERIFIED THEIR DETAILS?

Are they a supplier or customer you don't know, or a friend using a new account? Don't be afraid to spend time checking credentials, e.g by ask for further details or checking who they are with trusted contacts.

AM I BEING PUT ON THE SPOT?

A very effective social engineering tactic is to make the victim feel like they're being pushed into a corner, the only way out being to comply. Don't be afraid to say: "Leave that with me and I'll get back to you," and then check official policy or ask for help.

IS THIS TOO MUCH INFORMATION?

Skilled social engineers pick up tiny titbits of information to build a picture of your organisation. All information you disclose has value. Think before you share.

AM I FOLLOWING PROCEDURES?

Do you have a standard process by which to treat suspicious emails, such as reporting it to an IT help desk? Don't second-guess it; know your organisation's policies and follow them.

IS IT A BOGUS ADDRESS?

Can you verify they have the email address of the organisation they claim to work for? It might be bogus. Check the website and the typical email style its employees use. If it's an odd-looking internal email, check the corporate directory.

BE SAVVY ABOUT THE SOCIAL ENGINEER!

TOGETHER, WE'VE GOT IT COVERED

National Protective Security Authority